Software Challenges in Integrated Modular Avionics (IMA) System Certification

FAA SACO DER Seminar

November 4, 2003

Will Struck, FAA TAD TSS, will.struck@faa.gov

Presentation Overview

- **Overview and IMA System Example**
- **Program Issues**
- **IMA System Issues**
- **Complex Electronic Hardware Issues**
- **Software Challenges**
- **Aircraft and Integrated System Issues**
- **Certification Authority Challenges**
- **Lessons Learned and the Future**

Disclaimer

- ✍ Views and opinions expressed in this presentation are those of the presenter, and do not constitute or represent an FAA position or opinion.

Introduction

- ✍ Not all of the issues and challenges will be IMA system specific, however, the presentation will hopefully illustrate how “traditional” system, hardware and software issues can be amplified when a highly complex and integrated system is being proposed for certification, and the potential adverse impacts on maintenance and continued operational safety of the aircraft and IMA system in-service

Improvement over time

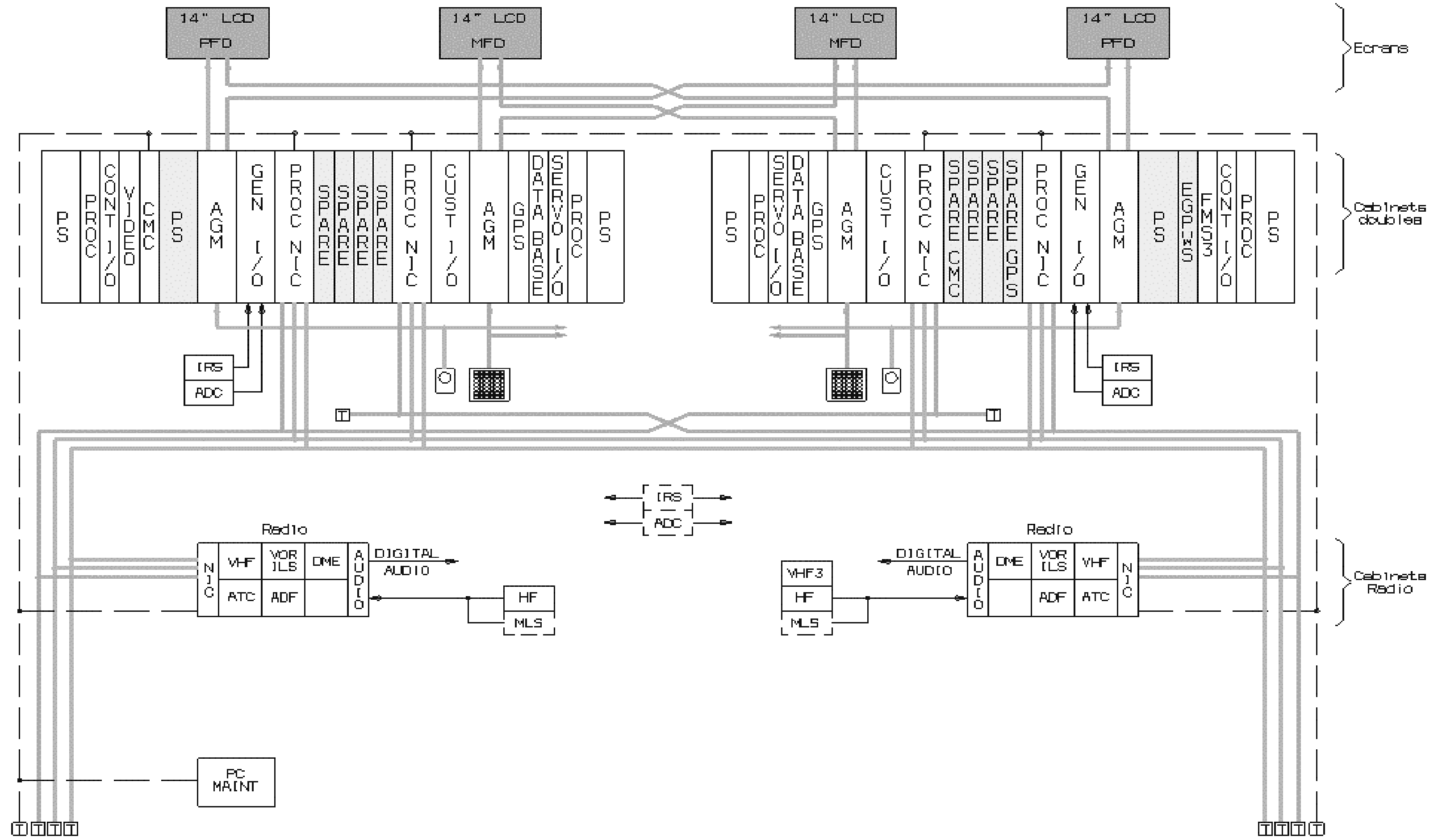
- Many of the issues and challenges resulted from over 3 years of being involved in the programs
- Resolution was achieved on most of the concerns

- A significant amount of improvement for the developer, the aircraft applicants and the certification authorities was achieved for this highly integrated and complex commercial aircraft IMA system

General IMA System Description

- **M**ultiple cabinets (5, 9, 16, 20 “slots”), single or dual power supplies, hosting single or multiple I/O cards (generic and custom), multiple aircraft function cards, most hosting multiple aircraft functions, with multiple buses (5) providing communications between cards, cabinets and other aircraft systems and sensors/actuators.
- **C**ommon processor cards, common operating system, common I/O (network, bus) “cards”, buses, power cards
- **C**ommon software: OS, Cabinet functions, I/O cards, card Core functions, HAL, PAL, PDD

Aircraft functions and sample layout



Program Issues (1 of 2)

- Multiple applicants for TC/ATC programs, domestic and international aircraft programs
- Applicant - Developer Coordination
- Multiple developer sites and organizations
- Experience on complex and highly integrated systems.
- Workload underestimated.
- Inadequate DER coverage
- Data availability and delivery

Program Issues (2 of 2)

- Simultaneous TC/ATC & TSO “approval”
- Simultaneous development of IMA HW TSO and AC
- JAA & FAA Common HW and SW Teams
- No Common systems team
- Underestimated maintenance as well?
- Schedule slides
- “Negotiated” Agreements

IMA Systems Issues (1 of 2)

- Complexity & integration of IMA system
- Missing sub-system and interface specs
- New unproven buses, power supplies, I/O devices
- Circuit Breakers, Resetting functions
- IMA system focal group formed late
- No conformed system integration V&V
- “Formal” testing on the aircraft

IMA Systems Issues (2 of 2)

- PSSA – aircraft & system level
- HW DAL and SW levels assignments
- Validating SSA assumptions
- Testing on non-conformed parts
- Integration of avionics and flight controls, fly-by-wire functions
- Many IMA functions aircraft specific (i.e., not common)

Complex Hardware Issues

- Simple versus Complex
- Alternative means “negotiated”
- TSO C153 and AC
- TAD PLD IP changed
- Relying on COTS HW
- Environmental Qualification Testing
- Failures & Changes late in program

Software Challenges (1 of 4)

- JAA and FAA Common Software Teams formed
- Reviews of Common software performed
- Inadequate planning by applicants, developer and CA
- Shortage of applicant and developer DER’s involved
- Lack of timely delivery & visibility of data to applicant
- Schedule delays – coordinating takes time.
- Interfaces and communications between groups
- “Issues” not propagated to other groups
- Microscope versus Big Picture perspectives, product and “pieces” scope issues
- Misinterpretations of DO-178B and other CA policy

Software Challenges (2 of 4)

- Software review Job Aid used inconsistently
- Reviewing informal, incomplete data
- Plans and standards finalized and released late
- “Alternative” means and methods proposed
- Incremental development
- Off-shore SW development and verification activities
- Software Review Job Aid not used at first
- Missing justification for assigned software levels
- Inadequate coordination and communication with safety
- Incomplete/inadequate system requirements

Software Challenges (3 of 4)

- Resolving deficiencies across development groups
- Lack of requirements flow between development groups
- Regression analysis/testing of SW changes late in program
- Formal SW V and V performed on aircraft
- Verification & assessing “pieces” w/o the whole
- Several versions of “Common” operating system
- Unique time and space partitioning protection
- Several versions of “Common” card support software

Software Challenges (4 of 4)

- Problem report categorization, analysis and resolution
- Legacy system software claims – unresolved deficiencies
- Deactivated code – executing
- Data coupling analysis, control coupling analysis
- Verification Independence
- Boot partitioning, extra functions
- Closure of Common Teams Review Findings
- Post TC activities promised – IOU's

Aircraft and Integrated Systems Issues

- Reduced functionality (multiple phase program) late in the program
- Concurrent TC and TSOA of “functions”
- Pre-TIA requirements list
- TIA Testing – software “maturity” prior to TIA
- Flight Testing
  - HW failures
  - Observed anomalies
  - etc.

Certification Authority Challenges (1 of 2)

- International CA and ACO Coordination
- HW TSO and AC being developed at same time
- Directorate policy being developed at same time
- Resolution of identified issues and agreement
- TSO process
- IMA Functional TSO’s
- “Credit” for approval on another aircraft
- Protecting company proprietary information
- “Level playing field”; most conservative

Certification Authority Challenges (2 of 2)

- Reduced functionality late in the program, disabling defective software functions
- Compliance with national policy
- Aural alerts interference, RNP/RNAV/VNAV, database integrity and accuracy, all electric displays including secondary, smart servos, smart air data probes, circuit breaker resets in ops procedures, flammability testing, etc.
- Closure late

Improvements (1 of 2)

- Ensure there are defined IMA system development plans, system architecture and safety features, SSA conducted, HW & SW safety requirements identified
- Identify & assess alternative MOC early
- Ensure DER coverage
- Defined CEH plans and MOC
- “Mature” software plans and standards
- Conduct real reviews, focus on big issues

Improvements (2 of 2)

- Don’t do developer’s job
- Don’t review informal data
- Insist on timely responses
- Document everything
- Insist on evidence
- Ensure IMA system integrated testing
- Ensure DER concurrence/approval

Summary

- IMA involvement useful for pointing out deficiencies in certification authority policy, industry standards and guidance, ACO standardization and FAA/FCAA harmonization for IMA systems.

- Coordination with AFS/AEG?

- What would we do better next time?

- Communicate – get clarity early

Questions and Discussion ...